CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

G.E., individually and on behalf of all others similarly situated,

Plaintiff,

vs.

STIIIZY INC.,

Defendant.

Case No. 2:25-cv-00490

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW BUSINESS & PROFESSIONS CODE § 17200, *et seq*.;
2. VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE § 56, *et seq*;
3. DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE §§ 1709, 1710;
4. NEGLIGENCE
5. BREACH OF EXPRESS WARRANTY
6. INVASION OF PRIVACY
7. UNJUST ENRICHMENT
8. VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT Cal. Civ. Code §§ 1750 *et seq*. ("CLRA")
9. DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

DEMAND FOR JURY TRIAL

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Plaintiff G.E.[1] individually and on behalf of all others similarly situated, ("**Plaintiff**") brings this Action against STIIIZY Inc. ("**STIIIZY**" or "**Defendant**"). Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein, after a reasonable opportunity for discovery.

INTRODUCTION

1. STIIIZY is a leading US cannabis brand that provides a range of premium cannabis products to consumers, ranging from potent indoor flower LIIIT to THC infused edibles, pod-based vaporizers, and extracts. Many consumers of STIIIZY's products utilize them to treat health concerns, such as chronic pain, nausea, and vomiting, including those related to serious diseases such as cancer and multiple sclerosis. STIIIZY frequently markets its products as promoting mental and physical health and well-being.

2. To purchase products from STIIIZY, customers are required to entrust STIIIZY with their highly sensitive and personally identifiable information ("**PII**") and, on some occasions, personal health information ("**PHI**") (collectively "**Private Information**"), which STIIIZY uses to engage in its usual business activities. STIIIZY understands that it has an enormous responsibility to protect the data it collected, assuring its customers that it "values your privacy"[2] and "implements security measures designed to protect your information from unauthorized access, disclosure or accidental loss or destruction."[3] Despite these assurances to its

[1] Plaintiff will be filing a Motion to Proceed Pseudonymously as part of this action.

[2] *Notice of Data Breach*, STIZZY, https://www.stiiizy.com/pages/notice-of-data-breach?srsltid=AfmBOopaL8d9szOjlv-QGULGYU9lod0KJ02mlxEYilBH5QiaSbKqQmSM (January 7, 2025).

[3] *Privacy Policy*, STIZZY, https://www.stiiizy.com/policies/privacy-policy (last visited Jan. 13, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

customers, STIIIZY failed to protect the very customer information it was entrusted, compromising the personal information of hundreds of thousands of its members (the "**Data Breach**"), announced by Defendant on January 7, 2025.[4]

3. STIIIZY failed to properly secure and safeguard the highly valuable, PII and PHI of its members, including members' names, addresses, dates of birth, drivers' license numbers, passport numbers, photographs, the signatures appearing on government ID cards, medical cannabis cards, transaction histories, and other personal information (collectively, "**Private Information**")[5]. STIIIZY also failed to comply with industry standards to protect information systems that contain Private Information and failed to provide timely and adequate notice to Plaintiff and other members of the Class that their Private Information had been accessed and compromised.

4. As a result of STIIIZY's inadequate security and breach of its duties and obligations, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiff and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (ii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiff's and Class Members' Private

[4] *Notice of Data Breach*, STIZZY, https://www.stiiizy.com/pages/notice-of-data-breach?srsltid=AfmBOopaL8d9szOjlv-QGULGYU9lod0KJ02mlxEYilBH5QiaSbKqQmSM (January 7, 2025).

[5] Lawrence Abrams, *STIIIZY data breach exposes cannabis buyers' IDs and purchases*, BLEEPING COMPUTER (Jan. 10, 2025), https://www.bleepingcomputer.com/news/security/stiiizy-data-breach-exposes-cannabis-buyers-ids-and-purchases/ (last accessed Jan. 13, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Information; (iv) the continued and certain increased risk that the Private Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; (vi) theft of their Private Information and the resulting loss of privacy rights in that information; (vii) diminution in value and/or lost value of Private Information, a form of property that Defendant obtained from Plaintiff and Class Members. This action seeks to remedy these failings and their consequences. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

5. Even the most fundamental Private Information, like names, dates of birth, and home addresses, when paired with other uniquely personalized data like drivers' license numbers, passport numbers, the signatures appearing on government ID cards, and the personal information included on medical cannabis cards, become especially valuable to cybercriminals to create seemingly legitimate, personalized phishing scams. This exfiltrated personal data, the full extent of which STIIIZY has failed to disclose to the public, allows hackers to gain a clear image of each individual and track their whereabouts, leading hackers to each victim's behavior and background. The combined exfiltrated data effectively provides criminals with a key to their personal lives, making it easy to match additional data, gaining access to their personal accounts and insight on their preferences. Hackers are now able to build a three-dimensional picture and thereby exploit STIIIZY's customers.

6. STIIIZY has disregarded the rights of Plaintiff and Class Members by, inter alia, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to prevent the

Data Breach; and failing to properly train its staff and employees on proper security measures.

7. In addition, STIIIZY failed to properly monitor its computer network and systems that housed the Private Information. Had it properly monitored these electronic and cloud-based systems, it would have discovered the intrusion sooner or prevented it altogether.

8. Defendant has also been unjustly enriched. When customers purchase Defendant's products, they are paying for not only the products themselves but also for proper data management and security. Defendant should have invested a greater portion of the monies received from Plaintiff and Class Members in proper data management and security, including proper and safe storage of Plaintiff' and Class Members' Private Information. Because Defendant failed to implement data management and security measures sufficient to protect that data and comply with industry standards, the principles of equity and justice demand that Defendant not be permitted to retain the money Plaintiff and Class Members paid Defendant for protection they did not receive.

9. Plaintiff brings this lawsuit on behalf of himself and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained. To remedy these violations of law, Plaintiff and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

I. PLAINTIFF

10. **G.E.:** Plaintiff G.E. is a natural person and resident of California. Plaintiff G.E. only allowed Defendant to maintain, store, and use his Private Information

because he reasonably expected that Defendant would use proper security measures to protect his Private Information and prevent its access by unauthorized third parties. As a result of this expectation, Plaintiff G.E. entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach. Had Plaintiff G.E. been informed of Defendant's insufficient data security measures to protect his Private Information, he would not have willingly provided his Private Information to Defendant.

11. Plaintiff G.E. has been a STIIIZY customer since at least October 2024 and purchased STIIIZY products at their location in Alameda, California - one of the four confirmed locations from which the Private Information has been exfiltrated.

12. In order to purchase cannabis from STIIIZY, Plaintiff G.E. was required to, and did, provide a driver's license to a STIIIZY employee, who input his name and other information, with a scan of his Driver's License, into STIIIZY's system.

13. Plaintiff typically paid by debit card, providing STIIIZY with his banking and other financial information when he purchased cannabis products from Defendant.

14. Plaintiff G.E. paid approximately $100 to receive cannabis products from STIIIZY's Alameda, California, dispensary. Plaintiff purchased the cannabis for his own personal use.

15. As a result of the Data Breach, Plaintiff has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

16. When Plaintiff's Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

17. Given the highly sensitive nature of the information involved, the Data Breach has also caused Plaintiff to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his Private Information. This highly sensitive information, which includes ***names, addresses, dates of birth, drivers' license numbers, passport numbers, photographs, the signatures appearing on government ID cards, medical cannabis cards, and transaction histories***, is now in the hands of criminals as a direct and proximate result of Defendant's misconduct. It is also possible that other forms of information not yet disclosed by Defendant were also lost in the breach.

18. As a result of the actual harm Plaintiff has suffered and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff to spend significant time and energy dealing with issues related to the Data Breach, including self-monitoring his accounts to ensure no fraudulent activity has occurred, dealing with a marked increase in spam texts and emails that occurred soon after the breach, and changing identifying information and passwords for his accounts. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

19. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff to suffer stress, fear, emotional distress, and anxiety.

20. Defendant acknowledged the risk posed to Class Members and their Private Information as a result of the Data Breach, explicitly stating that "STIIIZY values your privacy and deeply regrets that this incident occurred," encouraging customers to "remain vigilant against incidents of identity theft and fraud" and to "review account statements, and to monitor credit reports for suspicious or unauthorized activity."[6]

[6] *Notice of Data Breach*, STIZZY, https://www.stiiizy.com/pages/notice-of-data-breach?srsltid=AfmBOopaL8d9szOjlv-QGULGYU9lod0KJ02mlxEYilBH5QiaSbKqQmSM (January 7, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

II. DEFENDANT

21. **STIIIZY.** Defendant STIIIZY Inc. is incorporated in Delaware, with its principal place of business in the city of Los Angeles, California. Defendant conducts business, selling cannabis products to customers throughout the states of California, Washington, Nevada, Michigan, and Arizona.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367. Furthermore, even though Defendant claims that the only affected locations were in California, it is likely that due to the size of the breach, that the affected victims of the data breach – the Class Members – reside across the United States.

23. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant's principal place of business is located in this District from where its board of directors and/or officers direct Defendant's activities including to their actions and inactions leading to the data breach at issue; Defendant gains revenue and profits from doing business in this District; Class Members were affected by the breach from STIIIZY's actions and inactions directed from this District.

FACTUAL ALLEGATIONS

24. STIIIZY is a retailer of cannabis with tens of thousands of customers primarily in California. Defendant collects and processes the personal data of its customers. To purchase products from Defendant, customers are forced to entrust Defendant with their Private Information.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

25. The information collected and stored by Defendant includes, but is not limited to, ***names, addresses, dates of birth, drivers' license numbers, passport numbers, photographs, the signatures appearing on government ID cards, and medical cannabis cards***.

26. Defendant additionally has claimed that the Data Breach only impacted consumer profiles associated with the following STIIIZY locations:

- STIIIZY Union Square: 180 O'Farrell Street, San Francisco, CA
- STIIIZY Mission: 3326 Mission Street, San Francisco, CA
- STIIIZY Alameda: 1528 Webster St., Alameda, CA
- STIIIZY Modesto: 426 McHenry Ave., Modesto, CA.[7]

27. Defendant holds itself as a trustworthy company, which recognizes and values its customer's privacy and personal information and has repeatedly assured its customers that it "implements security measures designed to protect your information from unauthorized access, disclosure or accidental loss or destruction."[8] Defendant doubles down on its commitments, warranting that it "utilize[s] appropriate physical, technical and managerial safeguards designed to protect the information we collect."[9] Given that Defendant collects highly sensitive information like passport information, driver licenses, medical cards, social security numbers, dates of birth, and other sensitive data, Defendant should have implemented the necessary security measures, which would have prevented this Data Breach.

28. Plaintiff and other similarly situated customer's relied to their detriment on Defendant's uniform representations and omissions regarding data security,

---

[7] *Notice of Data Breach*, STIZZY, https://www.stiiizy.com/pages/notice-of-data-breach?srsltid=AfmBOopaL8d9szOjlv-QGULGYU9lod0KJ02mlxEYilBH5QiaSbKqQmSM (January 7, 2025).

[8] *Privacy Policy*, STIZZY, https://www.stiiizy.com/policies/privacy-policy (last visited Jan. 13, 2025).

[9] *Privacy Policy*, STIZZY, https://www.stiiizy.com/policies/privacy-policy (last visited Jan. 13, 2025).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

including Defendant's failure to alert customers that its security protections were inadequate, and that Defendant would forever store Plaintiff's and Class Members' Private Information, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.

29. Plaintiff and other similarly situated customer's trusted Defendant with their sensitive and valuable Private Information.

30. Had Defendant disclosed to Plaintiff and its other customers that its data systems were not secure and were vulnerable to attack, Plaintiff would not have purchased Defendant's products.

I. The Data Breach

31. At all material times, STIIIZY failed to maintain proper security measures despite its promises of safety and security to consumers.

32. On November 20, 2024, Defendant was notified by a vendor of point-of-sale processing services for some of its retail locations that accounts with its organization had been compromised by an organized cybercrime group. Defendant did not notify its customers then, nor make any announcements to alert them of this major security issue. Specifically, an investigation conducted by the vendor revealed that personal information relating to certain STIIIZY customers processed by the vendor was acquired by the threat actors at some point between October 10, 2024 - November 10, 2024. Despite being informed of the cyberattack on November 20, 2024, Defendant kept silent and chose not to notify the affected customers for several months.[10]

33. On or around January 7, 2025, Defendant finally began notifying some customers of the Data Breach via a posting on its website, including Plaintiff, when

[10] Lawrence Abrams, *STIIIZY data breach exposes cannabis buyers' IDs and purchases*, BLEEPING COMPUTER (Jan. 10, 2025), https://www.bleepingcomputer.com/news/security/stiiizy-data-breach-exposes-cannabis-buyers-ids-and-purchases/ (last accessed Jan. 13, 2025).

nearly two months had passed since Defendant learned of the unauthorized access.[11]

34. In its statement, Defendant does not disclose how many customers' Private Information was breached, leaving many consumers to speculate whether it is likely that their PII/PHI has been compromised. Instead, Defendant downplayed the extent of the Data Breach, and the likely harm affected victims may experience.

II. Data Breaches and the Market for PII/PHI

35. It should be no surprise that in today's digital economy the "world's most valuable resource is no longer oil, but data."[12] As such, personal information is a valuable property right.[13] Its value is axiomatic, considering the value of "big data" in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that personal information has considerable market value.

36. In a consumer-driven world, the ability to capture and use consumer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[14]

---

[11] *Notice of Data Breach*, STIZZY, https://www.stiiizy.com/pages/notice-of-data-breach?srsltid=AfmBOopaL8d9szOjlv-QGULGYU9lod0KJ02mlxEYilBH5QiaSbKqQmSM (January 7, 2025).

[12] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

[13] *See*, *e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[14] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

37. Indeed, an entire economy exists related to the value of personal data. In 2022, the big data technology market was valued at roughly $309 billion, and that value is expected to grow to $842 billion by 2023.[15]

38. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[16] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[17] OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military [record] is estimated to cost USD 55."[18]

39. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[19]

40. The U.S. Government Accountability Office (GAO) has concluded that it is common for data thieves to hold onto stolen data for extended periods of time

---

[15] Big Data Technology Market Research Report, Fortune Business Insights (Sept. 2023), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[17] *Id.* at 25.

[18] *Id.*

[19] U.S. Department of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2014 (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed December 5, 2024).

before utilizing it for identity theft.[20] In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[21]

41. PII is a valuable commodity for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000-$1,200 on the dark web[22] [23] and the legitimate data brokerage industry is valued at more than $250 billion.

42. When entities entrusted with personal data fail to implement industry best practices, cyberattacks and other data exploitations can go undetected for a long period of time. This worsens the ramifications and can even render the harm irreparable.

43. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data—including but not limited to identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[24]

---

[20] U.S. Government Accountability Office Report to Congressional Requesters, Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services, https://www.gao.gov/assets/700/697985.pdf (last accessed December 5, 2024).

[21] *Id.*

[22] Ryan Smith, *Revealed-how much is personal data worth on the dark web?*, INSURANCE BUSINESS MAGAZINE, https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx (last accessed December 5, 2024).

[23] Maria LaMagna, *The sad truth about how much your Google data is worth on the dark web*, MARKETWATCH (last accessed May 21, 2024). 17 Emily Wilson, The Worrying Trend of Children's Data Being Sold on the Dark Web, TNW (February 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark- web/ (last accessed December 5, 2024).

[24] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_ V2_combinedWEB.pdf (last accessed December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

44. PII has a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it.

45. Indeed, an entire economy exists related to the value of personal data. In 2022, the big data technology market was valued at roughly $309 billion, and that value is expected to grow to $842 billion by 2023.[25]

46. Defendant knew or should have known that Plaintiff's and Class Members' Private Information is valuable, both to legitimate entities, like Defendant, and to cybercriminals.

47. Defendant knew or should have known that Plaintiff and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of their data and systems, and that their valuable Private Information would be protected.

48. By collecting, using, selling, monitoring, and trafficking Plaintiff's and other customer's Private Information, and failing to protect it by maintaining inadequate security systems, failing to properly archive the Private Information, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiff and other STIIIZY customers.

III. Defendant's Duty to Safeguard Private Information

49. Defendant collects, receives, and accesses customers' extensive individually identifiable information. This Private Information includes names, drivers' license numbers, addresses, dates of birth, and other identifying information, as well as PHI in the form of health information such as medical cannabis cards.

50. Defendant was prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has

[25] Big Data Technology Market Research Report, Fortune Business Insights (Sept. 2023), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144

concluded that an entity's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

51. The FTC has brought enforcement actions against entities engaged in commerce for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all decision-making.[26]

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[27] The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

---

[26] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 5, 2024).
At https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 5, 2024).

[27] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-information.pdf (last accessed December 5, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

54. The FTC further recommends that entities not maintain PII or PHI longer than needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[28]

55. Furthermore, FTC requires that entities like Defendant conduct risk assessments, implement and periodically review access control, encrypt customer information, implement multi-factor authentication, dispose of customer information securely, maintain a log of authorized users' activity and keep an eye out of unauthorized access, train employees regarding security awareness, conduct audits, penetration testing, and system wide scans regularly to test for publicly known security vulnerabilities – all of which if properly implemented would have allowed Defendant to prevent this Data Breach.

56. Defendant failed to properly implement basic data security practices, allowing for this data breach to occur, victimizing thousands of people – by failing to adhere to many of the FTC protocols and allowing access to a hacker who was able to exfiltrate substantial amounts of consumer data. Defendant should have a multifaceted security protocol in place, including a program that adequately trains employees on recognizing and thwarting phishing and social engineering attacks, monitoring out-of-network emails, segmenting the network, flagging suspicious domain addresses or content, utilized multifactor authentication before allowing access to highly sensitive information, mandating strict compliance with these protocols; mandating regular archiving of email data/removal of sensitive data from emails to servers; avoiding exchanging any sensitive data for customers over the emails, simulating social engineering attempts to ensure compliance, increasing spam

[28] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 5, 2024).

filtering via email gateways, implementing strict policies regarding exchange of PII/PHI over emails, implementing and enforcing appropriate credential/key procedures including finger print recognition/physical key authentication; monitoring systems 24/7 for any suspicious activity, encrypting data over the email exchanges. Had Defendant maintained these and other proper protocols and regularly conducted audits to ensure its vulnerabilities and training, it would have prevented this Data Breach.

57. Plaintiff and Class Members provided their Private Information to STIIIZY with the reasonable expectation and mutual understanding that STIIIZY would comply with its obligations to keep such information confidential and secure from unauthorized access.

58. STIIIZY's failure to provide adequate security measures to safeguard members' Private Information is especially egregious because it operates in a field which has recently been a frequent target of scammers attempting to gain access to confidential PII/PHI.

IV. Impact of the Data Breach on Consumers

59. Plaintiff and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures that led to a data breach. This breach allowed hackers to access the Private Information, including ***names, addresses, dates of birth, drivers' license numbers, passport numbers, photographs, the signatures appearing on government ID cards, medical cannabis cards, and transaction histories*** of Plaintiff and the Class. Now that the Private Information has been accessed and absconded with, it is available for criminal elements to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

years."[29]

60. Plaintiff and Class Members are now vulnerable to a full gamut of cybercrimes, loss in value of their property, and have been forced to take remedial action, as listed below:

Digital Phishing Scams

61. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[30]

62. Defendant knew or should have known of the dangers of digital phishing scams. When Personal Information is employed in a social engineering scheme, criminals can gain unfettered access to individuals, or corporate databases, as the Data Breach itself evinces.

63. Defendant's customers are now more likely to become victims of digital phishing attacks because of the compromised information.

SIM-Swap

64. The data leak can also lead to SIM-swap attacks against Plaintiff and the Class Members. A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's phone number to the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks

---

[29] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf. (Last visited December 19, 2023).

[30] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Last visited December 19, 2023).

for the Class.

65. Defendant's customers are now more likely to become victims of SIM Swap attacks because of the released personal information.

Loss of Time

66. As a result of this breach, Plaintiff and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach. In addition, Plaintiff, as a result of the breach, has spent significant time and effort researching the breach, monitoring his accounts for fraudulent activity, and dealing with increased unsolicited emails and texts.

Threat of Identity Theft

67. As a direct and proximate result of Defendant's breach of confidence, and failure to protect Private Information, Plaintiff and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of Private Information that belongs to Plaintiff.

Out of Pocket Costs

68. Plaintiff is now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiff anticipates spending out of pocket expenses to pay for these services.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Diminution in Value of a Valuable Property Right

69. Because personal data is valuable personal property, market exchanges now exist where internet users like Plaintiff and Class Members can sell or monetize their own personal data.

70. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to legitimate marketers or app developers.[31] For example, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[32]

71. Accordingly, as a result of the Data Breach, Plaintiff lost the sale value of his Private Information and the opportunity to control how it is used. That a threat actor specifically targeted Defendant demonstrates just how valuable Plaintiff's Private Information can be to hackers and the significant value of Plaintiff's Private Information to cybercriminals.

Summary of Actual Economic and Noneconomic Damages

72. In sum, Plaintiff and similarly situated consumers were injured as follows:

i. Theft of their Private Information and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their Private Information;

iii. Loss of value of their Private Information;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiff's and other customers' Private Information that Defendant failed to adequately

[31] *See, e.g.*, *The Personal Data Revolution*, DATACOUP, https://datacoup.com/

[32] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

protect;

vi. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff is now exposed;

vii. Ascertainable out-of-pocket expenses and the value of Plaintiff's time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments for Defendant's products and/or services;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

V. Defendant Should Have Invested in Appropriate & Necessary Data Security

73. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks.

74. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that (1) cybercriminals were targeting companies who store personal health information, such as Defendant; (2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant; (3) cybercriminals were selling large volumes of Private Information and corporate information on Dark Web portals; and (4) the threats were increasing.

75. Had Defendant been diligent and responsible, it would have implemented the basic cyber security steps necessary to protect the Private Information in its possession, by addressing the key vulnerabilities:

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

- Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services;
- Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;
- Misconfigured devices/servers;
- Unencrypted data and/or poor encryption key management and safeguarding;
- Use of end-of-life (and thereby unsupported) devices, operating systems, and applications;
- Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;
- Failure to block malicious email; and
- Users succumbing to business email compromise (BEC) and social exploits.[33]

76. Considering the information and warnings readily available to Defendant before the Data Breach, Defendant had reason to be on guard and to increase data security to avoid an attack.

77. Prior to the Data Breach, Defendant thus knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Private Information could be accessed, exfiltrated and utilized by nefarious individuals as the result of a cyberattack.

78. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices; being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[34]

---

[33] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable (last accessed January 17, 2025).

[34] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES BUSINESS COUNSEL, FORBES (Jul. 30, 2021) available at

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

79. Defendant did not follow this advice; nor did it heed warnings from the U.S. Department of Health and Human Services as well as cybersecurity industry experts that the Everest ransomware gang, which was responsible for the cyberattack, was increasingly targeting the healthcare industry, which made Defendant a target as it had PHI.[35] Had Defendant properly prepared itself and its employees to comply with industry standards, this Data Breach would have been preventable.

CLASS ALLEGATIONS

80. Plaintiff brings this action on his own behalf and on behalf of all other persons similarly situated. The Class which Plaintiff seek to represent comprises:

> All persons whose Private Information was accessed, compromised, or stolen in the Data Breach announced by Defendant on January 7, 2025 (the "Class").

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

81. The Class is comprised of thousands of STIIIZY customers who have purchased items from STIIIZY in the past and were part of the Data Breach (the "Class Members"). The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

82. STIIIZY has claimed that "the incident only impacted consumer profiles associated with" four STIIIZY locations, all in California. Plaintiff reserves the right to seek to expand the class if it is found that the Data Breach involved STIIIZY

---

https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da (last accessed December 4, 2024).

[35] Lawrence Abrams, *STIIIZY data breach exposes cannabis buyers' IDs and purchases*, BLEEPING COMPUTER (Jan. 10, 2025), https://www.bleepingcomputer.com/news/security/stiiizy-data-breach-exposes-cannabis-buyers-ids-and-purchases/ (last accessed Jan. 17, 2025).

locations in the other states that it operates.

83. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code § 17200, *et seq*.;

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code § 17200, *et seq*.;

c. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code § 17200, *et seq*.

d. Whether Defendant's conduct is in violation of California Civil Code § 56, *et seq*.;

e. Whether Defendant's conduct is in violation of California Civil Code §§1709 and 1710;

f. Whether Defendant's failure to implement effective security measures to protect Plaintiff's and the Class's Private Information was negligent;

g. Whether Defendant breached express and implied warranties of security to the Class;

h. Whether Defendant represented to Plaintiff and the Class that it would protect Plaintiff's and the Class Members' Private Information;

i. Whether Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

j. Whether Defendant breached a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

k. Whether Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

l. Whether Defendant's conduct caused or resulted in damages to Plaintiff and the Class;

m. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

n. Whether Defendant knew or should have known that its systems, including but not limited to training protocols and policies, left it vulnerable to the Data Breach;

o. Whether Defendant adequately addressed the vulnerabilities that allowed for the Data Breach; and

p. Whether, as a result of Defendant's conduct, Plaintiff and the Class are entitled to damages and relief.

84. Plaintiff's claims are typical of the claims of the proposed Class, as Plaintiff and Class Members were harmed by Defendant's uniform unlawful conduct.

85. Plaintiff will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has retained competent and experienced counsel in class action litigation and other complex litigation.

86. Plaintiff and the Class have suffered injury because of Defendant's false, deceptive, and misleading representations.

87. Plaintiff would not have given his Private Information to Defendant but for the reasonable belief that Defendant would safeguard his data and Private Information.

88. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

used in class actions, and by internet publication, radio, newspapers, and magazines.

89. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

90. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

91. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

92. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class Members' claims, few, if any, Class Members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, Class Members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.*

(ON BEHALF OF THE CLASS)

93. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

A. "Unfair" Prong

94. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

95. Defendant's conduct as alleged herein does not confer any benefit to consumers. Mishandling this data shows blatant disregard for its customers' privacy and security.

96. Defendant's conduct as alleged herein causes injuries to consumers who do not receive goods or services consistent with their reasonable expectations. Specifically, Defendant's customers would not have reason to believe that simply doing business with Defendant would place their Private Information in the hands of cybercriminals.

97. Defendant's conduct as alleged herein causes injuries to its customers, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

98. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in law, including the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's

Consumer Privacy Act, Cal. Civ. Code § 1798.100.

99. Defendant's customers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

100. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

101. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

102. Defendant could have furthered its legitimate business interests in ways other than its unfair conduct.

103. Defendant's conduct threatens members by misleadingly advertising its purported "commitment" to protecting Private Information while exposing members' Private Information to hackers. Defendant's conduct also threatens other entities, large and small, who play by the rules. Defendant's conduct stifles competition, has a negative impact on the marketplace, and reduces consumer choice.

104. All of the conduct alleged herein occurs and continues to occur in Defendant's operations. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated consistently.

105. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

106. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff relied on and made his purchase decision in part based on Defendant's representations regarding its security measures and trusted that Defendant would keep his Private Information safe and secure. Plaintiff accordingly provided his Private Information to Defendant reasonably believing and expecting that his Private Information would be safe and secure. Plaintiff paid an unwarranted premium for the products he received.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Specifically, Plaintiff paid for goods from Defendant since Defendant represented that doing business with it would be secure and private, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to the Data Breach.

107. Plaintiff and the Class would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Plaintiff and Class Members seek an order mandating that Defendant implement adequate security practices to protect customers' Private Information. Additionally, Plaintiff and Class Members seek an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

B. "Fraudulent" Prong

108. California Business and Professions Code Section 17200, et seq. considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

109. Defendant's advertising and representations that it adequately protects consumer information is likely to deceive members of the public into believing that Defendant can be entrusted with Private Information, and that Private Information gathered by Defendant is not in danger of being compromised.

110. Defendant's representations about its commitments to data security, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

111. Defendant knew or should have known of its fraudulent conduct.

112. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

113. Defendant could have implemented robust security measures to prevent

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

the Data Breach but failed to do so.

114. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

115. Pursuant to Business & Professions Code Section 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive representations about the strength or adequacy of its security systems. Likewise, Plaintiff and the Class seek an order requiring Defendant to disclose such misrepresentations.

116. Plaintiff and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiff paid an unwarranted premium for the products he received. Specifically, Plaintiff believed that his information would be secure with Defendant when he did business with them, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to the Data Breach.

117. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer Private Information retained by Defendant. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, adopting adequate and robust training policies and protocols for all employees entrusted with access to Personal Information and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

118. California Business and Professions Code Section 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.,* 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

119. Defendant's unlawful conduct, as alleged in the preceding paragraphs,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

violates California Civil Code Section 1750, *et seq.*

120. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

121. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California common law.

122. Defendant knew or should have known of its unlawful conduct.

123. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

124. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

125. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

126. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

127. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff paid an unwarranted premium for Defendant's products, believing that Defendant would protect his PII and PHI from breach. Plaintiff would not have purchased the products, paying or overpaying for the products, if he had known that his purchase would put his Private Information at risk. Plaintiff and the Class would not have given Defendant their

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiff and Class Members seek an order mandating that Defendant implement adequate security practices to protect members' Private Information. Additionally, Plaintiff and the Class Members seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

128. No adequate remedy at law. Plaintiff and the Class are entitled to equitable relief as no adequate remedy at law exists.

129. Defendant has not yet implemented adequate protections to prevent a future data breach, nor has it given an adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

130. Injunctive relief is also necessary to prevent the members of general public from being misled by Defendant's misrepresentations regarding privacy and security of information;

131. The equitable relief under the UCL (and also under unjust enrichment discussed below) creates a straightforward cause of action for violations of law (such as statutory or regulatory requirements related to representations and omissions made with respect to Defendant's products). Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially eliminate possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

132. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, forcing an election of remedies at the initial pleadings stage, in the absence of completed discovery regarding class certification and merits, is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

COUNT TWO

VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CALIFORNIA CIVIL CODE SECTION 56, *et seq.*

(ON BEHALF OF THE CLASS)

133. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

134. Defendant is subject to the requirements and mandates of the CMIA because it is a "contractor" and/or "provider of health care" pursuant to Cal. Civ. Code § 56.06.

135. CMIA section 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

136. As a direct result of its negligent failure to adequately protect the data it collected from the Plaintiff and Class Members, Defendant allowed for a Data Breach which released the PII/PHI of Plaintiff and the Class Members to criminals and/or third parties.

137. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment."

138. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the [customers]' name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.050.

139. Defendant is in possession of affected individuals' medical information, as it has indicated that its customers' medical cannabis cards were lost in the data breach. Thus, information relating to the diagnosis and treatment of patients/customers, at minimum, was exposed in the data breach. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of Plaintiff by the third parties to whom the data was disclosed. Class Members' names, photographs, and addresses were included in the compromised data.

140. Defendant came into possession of Plaintiff's and Class Members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiff's and Class Members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, store, abandonment, destruction, or disposal of confidential medical information.

141. Defendant further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained Plaintiff's and Class Members' medical information, allowing and enabling a threat actor to view and access unencrypted PHI for Class Members.

142. Since Defendant maintained Plaintiff's and class members medical information in California, on California-based servers, where it was ultimately disclosed to third parties, CMIA equally applies to the entire affected Class. *See, e.g., Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023 U.S. Dist. LEXIS 158683, at *16 (N.D. Cal. Sep. 7, 2023) (holding that another statute, CIPA, could apply to non-residents of California, because the conduct at issue occurred in California).

143. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiff and class members have been injured and are entitled to compensatory

damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT THREE

DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710

(ON BEHALF OF THE CLASS)

144. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

145. Defendant knew or should have known that its internal systems were inadequate to protect Class Members' Private Information. Specifically, Defendant had an obligation to disclose to its customers that its internal systems were not adequate to safeguard their Private Information. Defendant did not do so. Rather, Defendant deceived Plaintiff and the Class by concealing the vulnerabilities in its systems.

146. Even after Defendant discovered the Data Breach had impacted sensitive Private Information, it concealed it, and waited nearly two months before announcing it to the public so consumers could know and take precautions against the Data Breach.

147. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiff and the Class.

148. California Civil Code §1709 mandates that in willfully deceiving Plaintiff

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

and the Class with intent to induce or alter their position to their injury or risk, Defendant is liable for any damages which Plaintiff and the Class thereby suffer.

149. As described above, Plaintiff and the Class have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Had Defendant been truthful about its security vulnerabilities or had promptly and adequately notified affected parties that their information had been compromised, Plaintiff and the Class would not have suffered some, if not all, of the harms attributable to the Data Breach. Specifically, Plaintiff and the Class have been subject to numerous attacks, including an increase in spam texts and other scam attempts. Defendant is liable for these damages as well.

COUNT FOUR

CALIFORNIA CONSUMER PRIVACY ACT, CALIFORNIA CIVIL CODE § 1798.100

(ON BEHALF OF THE CLASS)

150. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

151. Defendant boasts over 2 dozen locations in California alone as well as numerous cultivate, manufacturing, and distribution facilities throughout the state.[36]

152. Defendant STIIIZY also has significant revenue, with an estimated annual revenue between $100 Million to $1 Billion dollars, between 1,001-5,000 employees, and having recently received financing of $36,000,000 as part of its operations.[37]

153. STIIIZY is considered a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c) because on information and belief, it has an annual gross revenue exceeding $25 million and it buys, receives, sells, or shares personal information of

[36] *Assets*, STIIIZY, https://www.stiiizy.com/pages/assets (last accessed January 17, 2025).

[37] *STIIIZY Company Overview*, LEADIQ, https://leadiq.com/c/stiiizy/5d16634d1f0000ff0027160a, (last accessed January 17, 2025).

50,000 or more consumers, households, or devices.

154. Plaintiff's and Class Members' PII is "nonencrypted and nonredacted personal information" consisting of social security number, names, addresses and other sensitive personal information. Cal. Civ. Code § 1798.150(a)(1). The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1) because due to Defendant's failure to implement reasonable and necessary security measures, it enabled third party criminals to access personal information and thus, caused unauthorized sharing of Plaintiff's and the Class Members' personal information.

155. Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of Plaintiff's and Class Members' PII to protect said PII.

156. Defendant breached the duty they owed to Plaintiff and Class Members described above. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

157. Defendant's breach of the duty they owed to Plaintiff and the Class Members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff and the Class Members suffered damages, as described above and as will be proven at trial.

158. Plaintiff and the Class Members seek injunctive relief in the form of an order enjoining Defendant from continuing the practices that constituted their breach of the duty owed to the Plaintiff and Class Members as described above

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT FIVE

NEGLIGENCE

(ON BEHALF OF THE CLASS)

159. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

160. Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

161. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiff and Class Members, who were the foreseeable and probable victims of any inadequate security practices.

162. Defendant had a special relationship with Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach. Plaintiff and Class Members were compelled to entrust Defendant with their Private Information. At relevant times, Plaintiff and Class members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiff's and Class Members' Private Information it held.

163. Defendant knew or should have known that Plaintiff's and the Class Members' Private Information is information that is frequently sought after by criminals.

164. Defendant knew or should have known that Plaintiff and the Class

members would suffer harm if their Private Information was leaked.

165. Defendant knew or should have known that its security systems were not adequate to protect Plaintiff's and the Class Members' Private Information from a data breach.

166. Defendant knew or should have known that adequate and prompt notice of the Data Breach was required such that Plaintiff and the Class could have taken more swift and effective action to change or otherwise protect their Private Information. Defendant failed to provide timely notice upon discovery of the data breach. Class Members were informed of the data breach on January 7, 2025, with many not receiving actual notice. Defendant had learned of the data breach nearly two months prior, in November 2024.

167. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Class Members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintain adequate measures to detect a data breach when it occurred.

168. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

169. Plaintiff's and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. The leak of Plaintiff's and the Class Members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

170. Defendant's negligence was, at least, a substantial factor in causing Plaintiff's and the Class's Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Class Members' other injuries arising out of the Data Breach.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

171. The damages suffered by Plaintiff and the Class were the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiff's and Class Members' Private Information.

172. Defendant knew or should have known that its security for safeguarding Plaintiff's and Class Members' Private Information was inadequate and vulnerable to a data breach.

173. Defendant's negligence directly caused significant harm to Plaintiff and Members of the Class.

COUNT SIX

BREACH OF EXPRESS WARRANTY

(ON BEHALF OF THE CLASS)

174. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

175. Defendant made an express warranty to Plaintiff and Class Members that it is committed to protecting the Private Information entrusted to it. In order to purchase Defendant's products, Plaintiff and Class Members were required to provide their Private Information which they reasonably believed, based on Defendant's express representations, would be kept private and secure.

176. Defendant's express warranties regarding its security standards made to Plaintiff and the Class appear throughout its Privacy Policy.[38] The promise of security is associated with the offerings and products, and therefore becomes the basis of the bargain.

177. Plaintiff and the Class engaged in business with Defendant, including entrusting it with their Private Information, with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express

[38] *Privacy Policy*, STIZZY, https://www.stiiizy.com/policies/privacy-policy (last visited Jan. 13, 2025).

warranties made by Defendant on its website.

178. Defendant breached the express warranties made to Plaintiff and Class Members by failing to provide adequate security to safeguard Plaintiff's and the Class's Private Information. As a result, Plaintiff and Class Members suffered injury and deserve to be compensated for the damages they suffered.

179. Plaintiff and Class Members paid money to purchase products from Defendant. However, Plaintiff and Class Members did not obtain the full value of the advertised products. If Plaintiff and other Class Members had known that their Private Information would be exposed as a result of their purchasing the products, then they would not have purchased the products.

180. Plaintiff and the Class are therefore entitled to recover all available remedies for said breach of express warranty, as this Court deems proper.

COUNT SEVEN

INVASION OF PRIVACY

(ON BEHALF OF THE CLASS)

181. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

182. Plaintiff and Class Members had a reasonable and legitimate expectation of privacy in their Private Information that Defendant failed to adequately protect against compromise from unauthorized third parties.

183. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

184. Defendant failed to protect, and released to unknown and unauthorized third parties, the Private Information of Plaintiff and Class Members.

185. By failing to keep Plaintiff's and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully invaded Plaintiff's and Class Members' privacy by, among others, (i) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiff's and Class Members' Private Information without consent.

186. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider its actions highly offensive.

187. Defendant knew, or acted with reckless disregard of the fact that, organizations handling PII or PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

188. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, thereby causing Plaintiff and the Class Members undue harm.

189. Plaintiff seeks injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiff and Class Members. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the class.

COUNT EIGHT

UNJUST ENRICHMENT

(ON BEHALF OF THE CLASS)

190. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

191. Defendant funds its data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiff and Class Members.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

192. A portion of the payments made by or on behalf of Plaintiff and Class Members was to be used to provide the necessary level of data security.

193. Plaintiff and the Class conferred a monetary benefit on Defendant by purchasing the products from Defendant and in doing so provided Defendant with their most sensitive PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the products that were subject to the transaction and had their PII protected with adequate data security measures.

194. Defendant knew that Plaintiff and the Class conferred a benefit which it accepted, and through which Defendant was unjustly enriched. Defendant profited from these transactions and used Plaintiff's and the Class's PII and PHI for business purposes to increase their revenues.

195. Defendant enriched itself by saving the costs they reasonably should have spent on the necessary data security measures to secure Plaintiff's and the Class Members' PII and PHI. Instead of providing the necessary level of security that would have prevented the Data Breach, Defendant instead calculated to increase their own profits at the expense of Plaintiff and the Class, by using ineffective security measures, failing to pay money for the much needed training of their employees, failing to conduct the audits, implementing other security measures discussed above. Plaintiff and the Class suffered an injury as a direct and proximate resolute of Defendant's decision to prioritize its own profits over the requisite security and training.

196. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class, because it failed to implement appropriate data management and security measures as mandated by common law and statutory duties.

197. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information nor would they have done business with Defendant.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

198. Plaintiff and the Class have no adequate remedy at law as discussed above.

199. Defendant should be compelled to disgorge its profits and/or proceeds that it unjustly received as a result of having Plaintiff's and Class Members' PII/PHI, or alternatively, Defendant should be compelled to refund the amounts that Plaintiff and the Class overpaid for its goods.

COUNT NINE

VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT

Cal. Civ. Code §§ 1750 et seq. ("CLRA")

(ON BEHALF OF THE CLASS)

200. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

201. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "**CLRA**"), California Civil Code § 1750, et seq. This cause of action does not seek monetary damages currently and is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendant with notice required by California Civil Code § 1782.

202. Plaintiff and Class Members are "consumers," as the term is defined by California Civil Code § 1761(d) because they purchased products for personal, family, or household purposes from Defendant.

203. Plaintiff, Class Members and Defendant have engaged in "transactions," as that term is defined by California Civil Code § 1761(e), since Plaintiff, Class Members and Defendant entered into agreements and performed those agreements when they made purchases of goods from Defendant in exchange for payment.

204. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

and the conduct undertaken by Defendant was likely to deceive consumers.

205. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

206. Defendant violated this provision by representing that Defendant took appropriate measures to protect Plaintiff's and the Class Members' Private Information

207. As a result, Plaintiff and the Class Members were induced to provide their Private Information to Defendant.

208. As a result of engaging in such conduct, Defendant has violated Civil Code § 1770.

209. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendant from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

210. Plaintiff and the Class Members suffered injuries caused by Defendant's misrepresentations, because they provided their Private Information believing that Defendant would adequately protect this information.

211. Plaintiff and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

212. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiff and members of the Class.

COUNT TEN

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(ON BEHALF OF THE CLASS)

213. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

214. The Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., authorizes this

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

215. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

216. Defendant owes a duty of care to Plaintiff and Class Members which require it to adequately secure its Private Information when it chose to accept and store Plaintiff's and Class Members' Private Information.

217. Defendant still possesses Plaintiff's and Class Members' Private Information.

218. Defendant does not specify in the Data Breach notification posted on its website what specific and verifiable steps it has taken to prevent a similar breach from occurring again.

219. Plaintiff and Class Members are at risk of harm due to the exposure of their Private Information and the Defendant's failures to address the security failings that lead to such exposure.

220. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their Private Information.

221. Plaintiff and the Class, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' Private Information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through any account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

222. The Court can, and should, issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with the law and industry standards to protect Plaintiff's and Class Members' Private Information.

223. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of the Defendant's systems or networks. The risk of another breach is real, immediate, and substantial.

224. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, the Plaintiff and the Class will likely be subjected to fraud, identity theft, and other harms described herein. However, the cost to the Defendant of complying with an injunction by employing reasonable prospective data security measures is minimal given they have preexisting legal obligations to employ these measures.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, pray for judgment and relief on all cause of action as follows:

A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. An order:

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's failure to provide notice to all affected consumers);

b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through any account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the

confidentiality and integrity of Plaintiff's and Class Members' Private Information;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury for all claims.

DATED: January 17, 2025

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart

Ryan Clarkson, Esq.
Yana Hart, Esq.
Bryan P. Thompson, Esq.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Email: *rclarkson@clarksonlawfirm.com*
Email: *yhart@clarksonlawfirm.com*
Email:*bthompson@clarksonlawfirm.com*